ABSTRACT

A countermeasure for differential power analysis attacks on computing devices. The countermeasure includes the definition of a set of split mask values. The split mask values are applied to a key value used in conjunction with a masked table defined with reference to a table mask value. The set of n split mask values are defined by randomly generating n-1 split mask values and defining an nth split mask value by exclusive or'ing the table mask value with the n-1 randomly generated split mask values.